REMARKS

Claims 1-22 and 24 are pending, with claims 1, 12 and 22 being independent. Claims 12, 18, and 22 have been amended. No new matter has been added. Specifically, the subject matter of claim 18 has been added to claim 12 and the subject matter of claim 23 has been added to claim 22. Claim 23 has been cancelled. Reconsideration and allowance of the above-referenced application are respectfully requested.

Rejections Under 35 U.S.C. §103

Claims 1 to 8 and 11 to 23 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 5,983,350 issued to Minear (hereinafter "Minear"), and further in view of U.S. Patent No. 6,959,346 issued to Low (hereinafter "Low).

Claims 9 and 24 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Minear and Low, and further in view of U.S. Patent Publication No. 2004/0160903 by Applicant Gai (hereinafter "Gai").

Claim 10 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Minear and Low, and further in view of U.S. Patent No. 6,426,706 issued to King (hereinafter "King").

These rejections and their underlying rationale are traversed. Applicant's claims are allowable over any combination of these references. For example, the proposed Minear-Low combination does not teach or suggest each and every element of claim 1.[1] The Examiner states that "[Minear] does not specifically teach the use of two physically separate high-speed crypto systems, to process messages with two different formats."[2] The Examiner then relies on Low, arguing that "Low teaches a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption of a first format kind of message, a second high-speed crypto system physically separate from said first high-speed

[1] Initially, as noted by the Examiner in the 8/3/2007 Office Action, claim 1 does not define that the lower speed crypto system also carries out at least one function other than encryption and decryption. The Applicant, however, preserves the right to add this distinguishing feature to claim 1 and other claims during prosecution.
[2] Office Action dated 8/3/2007 at page 7, lines 10-11.

crypto system using dedicated hardware components for cryptographic encryption and decryption of a second format kind of message different than said first format kind of message"[3] because "Low's Fig. 4 and 5 and their associated text teach a system including multiple processors, and buffers, where each packet will have a header inserted, which identifies which processor the packet should be sent for processing."[4]

Admittedly, Low discloses multiple processors with each processor dedicated to perform a specific function, e.g., classification, cipher processing, and combining packets; the Low reference, however, Low does not teach or suggest a processor that performs **both cryptographic encryption and decryption**.[5] In fact, nowhere does Low teach or suggest having **two crypto systems** with each dedicated to operate cryptographic encryption and decryption on a different format kind of message. This is because having two crypto systems for performing cryptographic functions would be contrary to the object of Low, which is to "provide a flexible processor architecture for supporting encryption and other processing of data within a data stream."[6] Furthermore, when Low discloses that "a new cipher processor is easily added"[7] it merely refers to the flexibility of being able to upgrade any of the processors without affecting other processors. Low simply does not contemplate using two processors to perform the same function, i.e., cryptographic encryption and decryption.

One potential application of the system of claim 1 is to provide a number of different optimized and unoptimized encryption and decryption structures that can be used for different

---

[3] *Id.* at lines 16-21.
[4] Office Action dated 8/3/2007 at page 7, lines 13-15.
[5] *See, e.g.*, Claim 8 of Low, which states "wherein **respective processors** perform IP header manipulation and encryption;" see also, Claim 10 of Low, which states "A method of **encrypting or decrypting data packets** comprising: modifying a received packet to include control data which includes **a list of processes to be performed on the packet**; forwarding the packet from processor to processor through an interconnection including a buffer controller which responds to control data in the packets to determine a **processor of the plurality of processors dedicated for processing a process** in the list of processes; and in successive processors, performing the processes identified by the control data, including **an encryption or decryption process**."
[6] Col. 3, lines 54-56; see also, e.g., Col. 7, lines 19-25, which states that "Typically client processors 54 are **dedicated to a single form of processing** that is self contained and can be performed on a packet in isolation. **Cipher processing is one such process**. Thus, a **DES encryption engine** typically **forms a client processor** for receiving data, for encrypting the data, and for returning the encrypted data to the SPB." (emphases added); see also, e.g., FIG. 8 and Col. 8, lines 29-36, which states that "The next process is that process indicated by control 3, **3DES Encryption**. Client 84 provides this functionality. The super packet is provided to **client 84** where, as shown in FIG. 9b **encryption is performed and the function control 3 is marked as having been performed.**" (emphases added).
[7] Col. 6, lines 60-61.

items. Claim 1, defines first and second high speed crypto systems. These two crypto systems are used for different formats of messages. Since one crypto system is used for one format and another for another format, these formats of crypto systems can be very quickly handled in this hardware. As noted above, Low does not disclose this claimed subject matter of first and second high speed crypto systems, which use dedicated hardware components for cryptographic encryption and decryption of a special format. Thus, the proposed Minear-Low combination does not teach or suggest "a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption of a first format kind of message, a second high-speed crypto system physically separate from said first high-speed crypto system using dedicated hardware components for cryptographic encryption and decryption of a second format kind of message different than said first format kind of message" as recited in claim 1.

Therefore, claim 1 is patentably distinct from Minear and Low, either alone or in combination, and claim 1 should be allowable for at least the reasons discussed above.

In addition, amended independent claim 12 also recites "a high-speed crypto system formed of hardware encryption parts including a first high-speed crypto part using dedicated hardware components for cryptographic encryption and decryption of a first format kind of message, a second high-speed crypto part physically separate from said first high-speed crypto part, using dedicated hardware components for cryptographic encryption and decryption of a second format kind of message, different than said first format kind of message" and is thus patentably distinguishable over the proposed Minear-Low combination for analogous reasons to those discussed for independent claim 1. Furthermore, because claims 2-11, 13-21, and 24 depend generally from claim 1 or 12, these dependent claims are patentably distinguishable over the proposed Minear-Low combination for at least the reasons provided above.

In addition, the Examiner's response to Applicant's arguments with respect to claim 11 in the previous response is respectfully traversed.[8] Specifically, the Examiner asserts that "As packets traverse through different layers of the IP communication model (i.e. physical, data link, network layers), each layer adds and strips the header associated with that layer." With all due

[8] Office Action dated 8/3/2007 at page 4, lines 12-17.

respect, the well-known encapsulation processes performed on IP packets, however, do not **replace** the headers with a cryptographic header and then process the message **using the cryptographic header**.

Furthermore, contrary to the Examiner's contention that "Low's figure 4 and associated text clearly teaches removing and adding cryptographic headers,"[9] FIG. 4 of Low does not teach or suggest, e.g., removing a header associated with a network interface or protocol, replacing the removed header with a cryptographic header, processing the message based on the cryptographic header, and then regenerating a new header associated with the network interface or protocol. This is because FIG. 4 of Low merely discloses that the master processor inserts a header to the received packet; where the inserted header is indicative of classification, cipher processing, combining packets.[10] The inserted header in Low is not associated with network interface or protocol, and there is simply no disclosure in Low of removing any header associated with the network interface, let alone regenerating a new header associated with the network interface. In addition, nowhere is there disclosure of a cryptographic header in Low, let alone replacing the header associated with a network interface with a cryptographic header, as recited in claim 11.

For at least these reasons discussed above, Low does not teach or suggest an "encryption and decryption system [that] includes a portion which removes a header associated with the network interface, replaces said header with a cryptographic header, processes said message using the cryptographic header, and then generates a new header associated with the network interface." as recited in claim 11. Accordingly, claim 11 should be additionally allowable for these reasons.

In addition, amended independent claim 22 also recites "removing a header associated with a network protocol ...; ... encrypting the message fragment, using said encryption header; and regenerating the header associated with the network protocol" and is thus patentably distinguishable over the proposed Minear-Low combination for analogous reasons to those discussed for claim 11.

Thus, all the pending claims are allowable for at least the reasons provided above.

---

[9] Office Action dated 8/3/2007 at page 4, lines 16-17.
[10] *See, e.g.*, Low at col. 6, lines 38-40.

Concluding Comments

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicants ask that all claims be allowed. Please apply applicable charges, including $60.00 for the one-month extension fee, or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 12/3/07

John C. Phillips
Reg. No. 35,322

Fish & Richardson P.C.
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

10792305.doc